



Home Overview **Download** Docs
Volunteer People Donate!



Tor: Packages and source

Tor is distributed as [Free Software](#) under the [3-clause BSD license](#).

If you want Tor to become faster and more usable, please consider [making a donation to the Tor project](#).

The latest stable release is **0.1.2.13**, and the latest development release is **0.1.2.13**.

Subscribe to the [or-announce mailing list](#) to keep informed of security advisories and new stable releases (you will need to confirm via email):

There is also an [RSS feed](#) of the or-announce list at [gmane.org](#).

Warning: Want Tor to really work?

...then please don't just install it and go on. You need to change some of your habits, and reconfigure your software! Tor by itself is **NOT** all you need to maintain your anonymity. There are several major pitfalls to watch out for.

First, Tor only protects Internet applications that are configured to send their traffic through Tor — it doesn't magically anonymize all your traffic just because you install it. We recommend you use [Firefox](#) with the [Torbutton](#) extension.

Second, browser plugins such as Java, Flash, ActiveX, RealPlayer, Quicktime, Adobe's PDF plugin, and others can be manipulated into revealing your IP address. You should probably uninstall your plugins (go to "about:plugins" to see what is installed), or investigate [QuickJava](#), [FlashBlock](#), and [NoScript](#) if you really need them. Consider removing extensions that look up more information about the websites you type in (like Google toolbar), as they may bypass Tor and/or broadcast sensitive information. Some people prefer using two browsers (one for Tor, one for unsafe browsing).

Third, beware of cookies: if you ever browse without Tor and Privoxy and a site gives you a cookie, that cookie could identify you even when you start using Tor again. You should clear your cookies frequently. [CookieCuller](#) can help protect any cookies you do not want to lose.

Fourth, Tor anonymizes the origin of your traffic, and it encrypts everything inside the Tor network, but [it can't encrypt your traffic between the Tor network and its final destination](#). If you are communicating sensitive information, you should use as much care as you would on the normal scary Internet — use SSL or other end-to-end encryption and authentication.

Fifth, while Tor blocks attackers on your local network from discovering or influencing your destination, it opens new risks: malicious or misconfigured Tor exit nodes can

send you the wrong page, or even send you embedded Java applets disguised as domains you trust.

Be smart and learn more. Understand what Tor does and does not offer. This list of pitfalls isn't complete, and we need your help [identifying and documenting all the issues](#).

Platform	Package	Setup info
Windows	Tor & Privoxy & Vidalia bundle: 0.1.2.13 (sig) , 0.1.2.13 (sig) .	Windows instructions
Windows packages for experts	Windows download page	Windows instructions
Mac OS X 10.4 (Tiger) Universal Binary	Tor & Privoxy & Vidalia bundle: 0.1.2.13 (sig) , 0.1.2.13 (sig) .	OS X instructions
Mac OS X 10.3 (Panther)	Tor & Privoxy & Vidalia bundle: 0.1.2.13 (sig) , 0.1.2.13 (sig) .	OS X instructions
Mac OS X packages for experts	OS X download page	OS X instructions
Linux/Unix packages	Linux/Unix download page	Linux/Unix instructions
Source tarballs	0.1.2.13 (sig) , 0.1.2.13 (sig) .	<code>./configure && make && src/or/tor</code>

More Information

- Here is a [list of sites mirroring the Tor site](#). Here is a [page with torrents for each download above](#). You can also download the [Privoxy source](#) or [Vidalia source](#).
- See our [FAQ entry on verifying package signatures](#), which allows you to make sure you've downloaded the file we intended you to get.
- See the [developer documentation](#) for instructions on fetching Tor from SVN to get the latest development version. Note that this version may not work or even compile!

Stable releases

2007-04-23: Tor 0.1.2.13 features [some major anonymity fixes, such as safer path selection; better client performance; faster bootstrapping, better address detection, and better DNS support for servers; write limiting as well as read limiting to make servers easier to run; and a huge pile of other features and bug fixes](#). The bundles also ship with Vidalia 0.0.11.

2006-12-14: Tor 0.1.1.26 fixes [a serious privacy bug for people who have set the HttpProxyAuthenticator config option](#).

You can read the [ChangeLog](#) for more details.

[Webmaster](#) - Last modified: Wed Apr 25 13:14:57 2007 - Last compiled: Wed Apr 25 14:00:39 2007

This page is also available in the following languages: [Deutsch](#), [español](#), [suomi](#), [français](#), [Italiano](#), [??? \(Nihongo\)](#), [norsk](#), [polski](#), [Português](#), [??????? \(Russkij\)](#), [svenska](#), [??\(?\) \(Simplified Chinese\)](#).
How to set [the default document language](#).